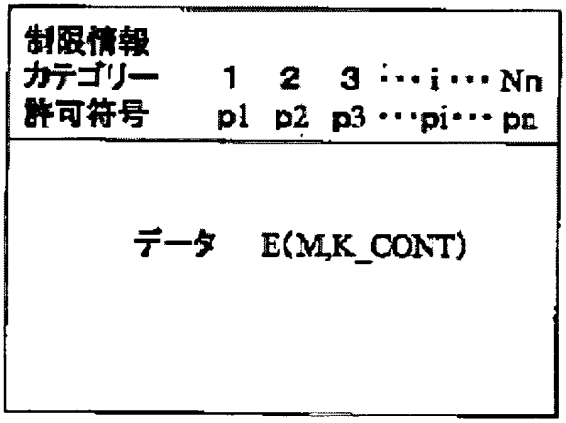
METHOD FOR DATA RECORDING AND READOUT, RECORDING DEVICE, READOUT DEVICE, AND WRITING DEVICE

Publication number: JP2000341265
Publication date: 2000-12-08
Inventor: KATSUTA NOBORU; KAWADA KOJI; HARADA TOSHIHARU; TATEBAYASHI MAKOTO
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: ***G06F12/14; G06F3/06; G06F21/24; G11B20/10; G11C16/02; H04L9/10;*** **G06F12/14; G06F3/06; G06F21/00; G11B20/10; G11C16/02; H04L9/10;** (IPC1-7): H04L9/10; G06F3/06; G06F12/14; G11B20/10; G11C16/02
- european:
Application number: JP19990149892 19990528
Priority number(s): JP19990149892 19990528

Abstract of **JP2000341265**

PROBLEM TO BE SOLVED: To make it difficult to make an illegal machine by reproducing contents data while ignoring permission information by recording data, ciphered on the basis of a key or recording data ciphering generated on the basis of recording and readout limitation information and a recording media key provided for recording equipment, and the recording and readout limitation information. SOLUTION: Data to be recorded are given a permission code of transmission and reception limitation information for respective categories. The categories may be the equipment number of equipment connected to equipment which records the data. The permission code is given for every category; and 0 indicates permission and 1 indicates nonpermission. The data are ciphered by using as a ciphering key K-CONT calculated from a function (f) depending upon the recording medium key Km of the recording equipment in addition to the permission information P. The function (f) may be a function which employs as an arithmetic result the output obtained by inputting P and Km as a key for block ciphering and a data input.



P={p1 ,p2,p3 ,・・・,pi,・・・, pn}:コンテンツ送受信先制限情報
K_CONT = f(P,K_m):コンテンツ暗号化鍵
f():コンテンツ鍵生成関数
pi = [0 許可 / 1 不許可]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－341265
(P2000－341265A)
(43)公開日　平成12年12月8日(2000.12.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
H04L	9/10		H04L	9/00	621Z　5B017
G06F	3/06	304	G06F	3/06	304M　5B025
	12/14	320		12/14	320B　5B065
G11B	20/10		G11B	20/10	H　5D044
G11C	16/02		G11C	17/00	601P　5J104

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

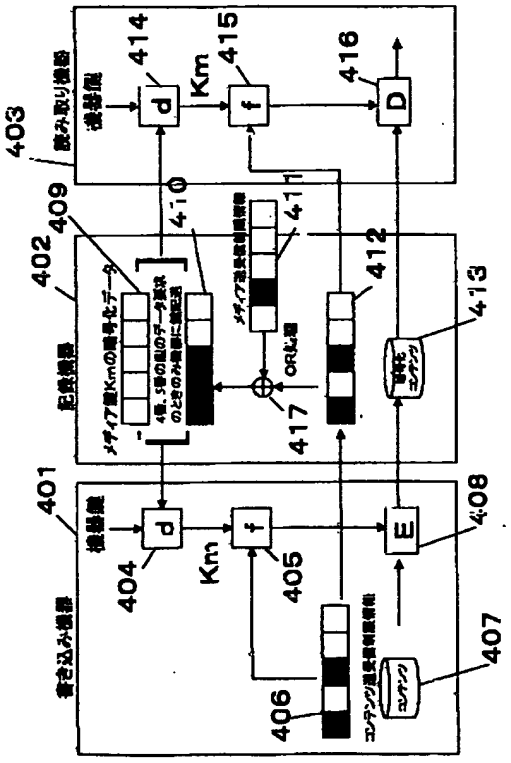
(21)出願番号　特願平11－149892
(22)出願日　平成11年５月28日(1999.5.28)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　勝田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　河田　浩嗣
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　データ記録および読み出し方法および記録装置および読み取り装置および書き込み装置

(57)【要約】
【課題】　本発明は、データの記録および読み出しに際してデータ作成者が許可した機器からだけに記録、読み出しを許すデータ記録方法および読み出し、書き込み方法および装置を提供する。
【解決手段】　データにデータが記録された機器から書き込み読み出しを許す機器についての許可情報をのせ、記録機器では、機器内にある許可情報とデータにある許可情報の両方から判断して読み書きを許す。さらにデータ記録に際しては、記録機器にあるメディア鍵とデータにある許可情報に依存した暗号化鍵でデータを暗号化する。



【特許請求の範囲】

【請求項１】データをその記録者が意図したものにのみ読み出し可能にするためのデータ記録機器へのデータ記録方法において

複数の読み出しおよび書き出し対象に対する記録および読み出し制限情報と記録する記録機器に設けられた記録メディア鍵とに基づき記録データ暗号化用鍵を生成し、前記暗号化鍵に基づき記録するデータを暗号化処理したのち、

前記暗号化されたデータと前記記録および読み出し制限情報を記録するデータ記録方法。

【請求項２】さらに記録メディア鍵は、記録機器より暗号化されたものを受信し、前記暗号化された記録メディア鍵を所持する機器鍵で復号処理して記録メディア鍵を生成することを特徴とする請求項１記載のデータ記録方法。

【請求項３】読み出し要求を受けたデータについて、そのデータに記述された送信制限情報と機器で所持する機器鍵で暗号化された記録メディア鍵をデータが記録されている記録機器より読み出し、前記送信制御情報と記録メディア鍵に基づき記録データに施された暗号を復号する復号鍵を生成し、

前記復号鍵に基づき読み出しデータを復号処理することを特徴とするデータ読み出し方法。

【請求項４】データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録するデータ内にあるデータ送受信先制限情報記憶部を具備し、

データ記録時、記録データにあるデータ送受信先制限情報を保持し、メディア鍵暗号化データについての読み出しリクエスト受信時、前記保持したデータ送受信先制限情報とメディア内送受信先制限情報記憶部にあるメディア内送受信先制限情報に基づき暗号化データ記憶部内のメディア鍵暗号化データ送出を制御し、データ記録時に、前記記録データより読み出し保持した送受信先制限情報を記録データとともに記録することを特徴としたデータ記録装置。

【請求項５】データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録または記録データあるデータ送受信先制限情報記憶部を具備し、

記録されたデータ出力時、読み出し要求データについてそのデータと送受信先制限情報を記録または読み出し対象データに関する送受信先制限情報として読み出し保持し、読み出し機器からのメディア鍵暗号化データの要求信号に対し、指示されたメディア鍵暗号化データについて、前記読み出し保持した対象データに関する送受信先制限情報とメディア内送受信先制限情報記憶部にある制限情報に基づき送出制御することを特徴とするデータ記録装置。

【請求項６】メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されることを特徴とする請求項４記載にデータ記録装置。

【請求項７】メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されることを特徴とする請求項６記載にデータ記録装置。

【請求項８】書き込みデータを暗号化するデータ暗号化手段と機器に付与された機器鍵を記憶する機器鍵記憶手段を具備し、

データ書き込み時、書き込みデータについての送受信先制限情報を送信し、機器鍵記憶手段に所持している機器鍵によって暗号化された鍵暗号化データを記録機器に要求し、要求にしたがって鍵暗号化が送出されきた場合のとき、前記鍵暗号化データを復号してメディア鍵情報を生成し、前記送信した書き込みデータに関する送受信先制限情報に基づきデータ暗号化鍵を生成し、

前記データ暗号化鍵によりデータをデータ暗号化手段で暗号化処理して記録機器に送出することを特徴とするデータ書き込み装置。

【請求項９】読み出しデータを暗号復号化処理する暗号化復号処理手段と機器鍵記憶手段と機器鍵および入力データにより読み出しデータを暗号復号化する暗号復号化鍵を生成制御する制御手段を具備し、

データ読み出し時、制御手段は、その読み出しデータを記録機器に指定し、さらに機器鍵記憶手段内にある機器鍵で暗号化された記録メディア鍵暗号化データ送信を記録機器に要求し、その結果、送信されてきた記録メディア鍵暗号化データを機器鍵に基づき復号処理して記録メディア鍵を生成し、さらに読み出しデータに対応した送受信先制限情報を記録機器より受信し、前記生成した記録メディア鍵と送受信先制限情報に基づきデータ復号鍵を生成することを特徴とするデータ読み出し装置。

【請求項１０】データを書き込みおよび読み出し可能な記録機器において、

記録機器に接続機器を限定する送受信先限定情報記憶手段と記録されるデータに付加された書き込み機器または読み出し機器を限定する送受信先限定情報読み取り手段を具備し、

書き込み機器および読み取り機器が接続され、データを書き込みあるいは読み取り処理される際、前記送受信先限定情報記憶手段に記憶された送受信先限定情報と前記送受信先限定情報読み取り手段で読み取ったデータに付

加された送受信先限定情報に基づき、データの記録および送出を制御することを特徴とするデータ記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音楽データや映画などの映像データなど著作権者が不正なデータの複製を拒否しているデータについて、録画や録音機器で不正に複製されることを防ぐためのデータ記録方法およびその読み出し方法および書き込み方法とその装置に関するものである。

【０００２】

【従来の技術】従来の録画機器や録音機器における著作権を保護するものとしては、たとえば、ディジタルオーディオのシリアルインターフェイスにおけるシリアルコピーマネージメントがある。これは、複製の許可情報をチャンネルステータス信号上に載せたものであるが、その情報が容易に改ざん可能であった。それを改善する方法としてたとえば、特願平４－１５７７１８号公報にコピーの許可情報記述方法についての記述がある。図１１は、従来の記録および伝送時許可情報記述方法の説明図である。同図において、許可コードは、それぞれのカテゴリー毎に設けられており、複製の許可不許可は、各カテゴリー内のコード１およびコード２の存在よって表現される。コード２は、コード１を一方向性の関数で処理した結果選られる値になっており、コード２からコード１を算出することは困難になっている。

【０００３】したがって、特定のカテゴリーについて複製を許可しない場合、コード１を取り除くことで不許可を表現する。そうすることで不許可を示す状態からコード１を生成して許可を示す情報を付加することは困難である。また、コード２に関するすべてのデータよりコンテンツデータを暗号化する暗号化鍵を生成し、コンテンツを暗号化しているため、複製許可情報を改ざんするとコンテンツデータを複製するための復号鍵を生成できなくなるため、許可情報を不正に改ざんできなくすることが出来る。

【０００４】

【発明が解決しようとする課題】しかしながら、前記従来の許可情報の記述方法では、コンテンツデータを暗号化する暗号化鍵を生成するパラメータが許可情報内に存在するため、暗号化鍵生成方法および暗号化アルゴリズムが秘密であることにのみ不正なコンテンツデータの解読に対する安全性が依存してしまう問題があった。すなわち、特定のカテゴリーにおけるコード１とコード２の関係を無視してもコード２からコンテンツデータ暗号データを復号することは可能であり、特定のカテゴリーの機器が不正な機器を作って自分のカテゴリーで許可されていないものまでも再生し不正することが可能である問題があった。

【０００５】以上のような問題点を鑑み本発明は、記録データだけからでは、許可情報を無視してコンテンツデータを再生し、不正な機器作ることが困難なデータ記録方法および読み出し方法、およびその装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】前記課題を解決するために本発明は、データをその記録者が意図したものにのみ読み出し可能にするためのデータ記録機器へのデータ記録方法において複数の読み出しおよび書き出し対象に対する記録および読み出し制限情報と記録する記録機器に設けられた記録メディア鍵とに基づき記録データ暗号化用鍵を生成し、前記暗号化鍵に基づき記録するデータを暗号化処理したのち、前記暗号化されたデータと前記記録および読み出し制限情報を記録するものである。

【０００７】また、本発明は、読み出し要求を受けたデータについて、そのデータに記述された送信制限情報と機器で所持する機器鍵で暗号化された記録メディア鍵をデータが記録されている記録機器より読み出し、前記送信制御情報と記録メディア鍵に基づき記録データに施された暗号を復号する復号鍵を生成し、前記復号鍵に基づき読み出しデータを復号処理するものである。

【０００８】また、本発明は、データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録するデータ内にあるデータ送受信先制限情報記憶部を具備し、データ記録時、記録データにあるデータ送受信先制限情報を保持し、メディア鍵暗号化データについての読み出しリクエスト受信時、前記保持したデータ送受信先制限情報とメディア内送受信先制限情報記憶部にあるメディア内送受信先制限情報に基づき暗号化データ記憶部内のメディア鍵暗号化データ送出を制御し、データ記録時に、前記記録データより読み出し保持した送受信先制限情報を記録データとともに記録するデータ記録装置の構成である。

【０００９】また、本発明は、データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録または記録データあるデータ送受信先制限情報記憶部を具備し、記録されたデータ出力時、読み出し要求データについてそのデータと送受信先制限情報を記録または読み出し対象データに関する送受信先制限情報として読み出し保持し、読み出し機器からのメディア鍵暗号化データの要求信号に対し、指示されたメディア鍵暗号化データについて、前記読み出し保持した対象データに関する送受信先制限情報とメディア内送受信先制限情報記憶部にある制限情報に基づき送

出制御するデータ記録装置の構成である。

【0010】本発明は、メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されるデータ記録装置の構成である。

【0011】また、本発明は、メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されるデータ記録装置の構成である。

【0012】また、本発明は、書き込みデータを暗号化するデータ暗号化手段と機器に付与された機器鍵を記憶する機器鍵記憶手段を具備し、データ書き込み時、書き込みデータについての送受信先制限情報を送信し、機器鍵記憶手段に所持している機器鍵によって暗号化された鍵暗号化データを記録機器に要求し、要求にしたがって鍵暗号化が送出されきた場合のとき、前記鍵暗号化データを復号してメディア鍵情報を生成し、前記送信した書き込みデータに関する送受信先制限情報に基づきデータ暗号化鍵を生成し、前記データ暗号化鍵によりデータをデータ暗号化手段で暗号化処理して記録機器に送出するデータ書き込み装置の構成である。

【0013】また、本発明は、読み出しデータを暗号復号化処理する暗号化復号処理手段と機器鍵記憶手段と機器鍵および入力データにより読み出しデータを暗号復号化する暗号復号化鍵を生成制御する制御手段を具備し、データ読み出し時、制御手段は、その読み出しデータを記録機器に指定し、さらに機器鍵記憶手段内にある機器鍵で暗号化された記録メディア鍵暗号化データ送信を記録機器に要求し、その結果、送信されてきた記録メディア鍵暗号化データを機器鍵に基づき復号処理して記録メディア鍵を生成し、さらに読み出しデータに対応した送受信先制限情報を記録機器より受信し、前記生成した記録メディア鍵と送受信先制限情報に基づきデータ復号鍵を生成することを特徴とするデータ読み出し装置の構成である。

【0014】また、本発明は、データを書き込みおよび読み出し可能な記録機器において、記録機器に接続機器を限定する送受信先限定情報記憶手段と記録されるデータに付加された書き込み機器または読み出し機器を限定する送受信先限定情報読み取り手段を具備し、書き込み機器および読み取り機器が接続され、データを書き込みあるいは読み取り処理される際、前記送受信先限定情報記憶手段に記憶された送受信先限定情報と前記送受信先限定情報読み取り手段で読み取ったデータに付加された送受信先限定情報に基づき、データの記録および送出を制御するデータ記録装置の構成である。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について図1から図10を用いて説明する。

【0016】図1は、本実施の形態における記録データの記録時におけるデータ構成の説明図である。同図において、記録されるデータには、各カテゴリーに対する送受信の制限情報の許可符号が付与される。このカテゴリーは、このデータが記録されている機器に接続される機器の機器番号でもよいし、機器に与えられている鍵の番号などである。許可符号は、各カテゴリー毎に与えられ、それぞれ0が許可、1が不許可を示す。データは、この許可情報Pに加えて記録されている記録機器にある記録メディア鍵Kmに依存した関数fにより算出されたK_CONTを暗号化鍵として暗号化する。関数fは、たとえば、ブロック暗号の鍵およびデータ入力にPおよびKmを入力してその出力を演算結果とするものでよい。

【0017】以上のように構成されたデータにおいては、各カテゴリーに示された許可コードは、データを暗号化する暗号化鍵を生成するパラメータになっているため、改ざんするとデータを復号するための鍵が作れなくなるため改ざんできない。また、記録メディア鍵Kmがデータ上に存在しないため、図1に示すデータを伝送路で盗聴あるいは記録機器からコピーされても暗号化されたデータを復号するための鍵を得ることができないため、データを再生できず不正な複製の作成を困難にできる。したがって、許可情報Pにしたがって許された機器へ記録メディア鍵Kmを伝送し、図1に示されるデータを送信記録するすべての記録、読み出し方法およびそれを実現する機器に本発明が適応できる。

【0018】図2は、本発明の実施の形態における記録機器およびそれにデータを書き込む書き込み機器の構成図である。同図において1は、データ書き込み機器、2は、データ記録機器、3は、書き込み機器1に与える機器鍵を記憶する機器鍵記憶部、4は、書き込み機器1と記録機器2での伝送路におけるデータの入出力制御を行う入出力制御部、5は、コンテンツデータを暗号化処理する暗号化処理部、6は、記録機器へ記録するデータを書き込み機器側で記録しているコンテンツ記録部、7は、図1の示した各カテゴリーの機器に与えられる機器鍵に基づきそれぞれ暗号化されてメディア鍵を記憶する鍵暗号化データ記憶部、8は、記憶機器内にあらかじめ与えられた各カテゴリーへの送受信の制限情報を記憶するメディア内送受信先制限情報記憶部、9は、送信されてくるコンテンツの送受信先制限情報を一時保持するコンテンツ送受信先制限情報記憶部、10は、書き込み機器との入出力制御部、11は、データ記録部である。

【0019】以上の構成において、以下その動作を説明する。まず、書き込み機器1は、PCなどのような内部で生成あるいはネットワーク等を介して取り込んでコンテンツデータをハードディスクなどの記録部に蓄えたものをメモリーカードへなどの記録機器へ記録するような場合が考えられる。したがって、書き込み機器と記録機器間の基本的なデータのそう受信は、たとえば、現在の

ＰＣとメモリカード間で行われている方法など一般に公知な方法を用いて行えるため、機器間を流れる情報について詳細に説明する。図２において、書き込み機器１と記録機器２間のデータ送受信は、入力制御部４および入力制御部１０で行われる。

【００２０】図６は、入力制御部４および１０で行われる処理フローを示した説明図である。同図において２０１は、書き込みリクエストおよびコンテンツ送受信先制限情報送出処理、２０２は、鍵暗号化データリクエスト番号送出処理、２０３は、記録メディア鍵復号処理、２０４は、コンテンツ暗号化鍵生成処理、２０５は、コンテンツ暗号化送出処理、２０６は、コンテンツ送受信先制限情報読み取り処理、２０７は、リクエスト番号有効性確認処理、２０８は、メディア鍵暗号化データ送出処理、２０９は、コンテンツデータ記録処理である。同図で左側に示された処理が図２における入出力制御処理４の処理であり、右側が入出力制御処理１０の処理である。まず、入出力制御部４は、記録機器２へ記録するため、書き込みリクエスト信号ともにコンテンツ記録部６より送信するコンテンツに対するコンテンツ送信先制限情報Ｐを読み出し、入出力制御部１０へ送信する。入出力制御部１０は、コンテンツ送受信先制限情報記憶部９へ記録する。次に、入力制御部４は、メディア鍵暗号化データリクエスト番号送出処理２０２において、機器鍵記録部３に記録された鍵が対応しているカテゴリー番号をリクエスト番号として入出力制御部１０へ送出する。次にリクエスト有効性確認処理２０７でコンテンツ送受信先制限情報記憶部９とメディア内送受信先制限情報記憶部８内のデータに基づき各カテゴリーに対する許可内容を確認する。図５は、メディア内送受信先制限情報Ｐｄの説明図である。図１におけるＰと同様に各カテゴリーに対して記録機器製造時に送受信を禁じたカテゴリーについて不許可の符号を与えたものである。図８は、コンテンツ送信先制限情報とメディア送受信先制限情報から送受信先の制限情報Ｐｄを算出する処理の説明図である。Ｐｃｄの各カテゴリーに対する要素は、ＰおよびＰｄの各要素のＯＲ処理によって生成される。そして、このように算出されたＰｃｄに基づいてリクエスト番号に対応するカテゴリーの許可符号が０であれば、許可あり判定し、メディア鍵暗号化データ送出処理２０８進み、そうでないときは、許可が否決されたとして処理を終了する。図９は、カテゴリー数が６の場合での具体的な送受信先制限情報Ｐｃｄの算出例の説明図である。コンテンツ側でカテゴリー１と４と６について不許可であり、メディア側でカテゴリ４と５について不許可であるとき、送受信先制限情報は、カテゴリー２と３のみ０となり許可をしめすことになる。

【００２１】図６のフローに戻って、メディア鍵暗号化データ送出処理２０８では、リクエスト番号に対応するカテゴリーに番号のメディア鍵暗号化データをメディア鍵暗号化データ記憶部７より選択して送出する。図４は、メディア鍵暗号化データの説明図である。各カテゴリーに対するデータは、記録メディア鍵Ｋｍをそれぞれのカテゴリーｉに付与された機器鍵Ｓｉで暗号化されたデータになっている。したがって、リクエストされたカテゴリー番号の鍵を用いれば、復号処理によりＫｍが生成できるデータが選択され送出される。

【００２２】記録メディア鍵復号処理２０３では、送られてきたメディア鍵暗号化データを機器鍵記憶部３にあるデータに基づき復号処理してＫｍを得る。次に、コンテンツ暗号化鍵生成処理２０４では、ＫｍとＰよりｆ（Ｐ Ｋｍ）を演算処理してコンテンツ暗号化鍵Ｋ＿ＣＯＮＴを生成する。そしてコンテンツ暗号化送出処理２０５では、コンテンツ記録部６より書き込むデータを暗号化処理部５に送り、コンテンツ暗号化鍵Ｋ＿ＣＯＮＴにより暗号化したデータを入出力処理部４を介して入出力処理部１０へ送出する。入出力処理部１０では、コンテンツデータ記録処理２０９で、送信されてきたデータにコンテンツ送受信先制限情報記憶部９に記録されたデータをコンテンツ送受信制限情報を付加して図１に示したデータとして記録する。

【００２３】以上のような動作により、書き込み機器および記録機器間では、図１で示したデータと書き込み機器鍵で暗号化された記録メディア鍵Ｋｍであるため、許可されたカテゴリーの機器以外にとっては、たとえば、通信路を盗聴したとしてもコンテンツを再生することが困難であり不正な複製を生成することができないようにできる。

【００２４】また、記録機器内にも送受信先制限情報を設けることにより、コンテンツおよび記録機器に入れられたどちらか最新の許可情報を有効にすることができ、より高い著作権保護能力が実現できる。すなわち、非常に以前に送信されたデータにつけられた送受信先制限情報では、数年たって、その後に作られた不正な機器については、それを不許可にすることが困難であるが、記録機器側により新しい制限情報があれば、コンテンツの流通後に発覚した不正機器についても排除が可能になる。また、逆に古い記録機器には、制限状態がほとんどないが、新しいコンテンツを記録された制限情報に基づいてコンテンツ側で排除したいカテゴリーを指定することでより高い著作権保護が実現できる。

【００２５】図３は、記録機器からの読み出しを行う読み出し機器と記録機器の構成を示した構成図である。同図において、１０１は、読み出し機器、１０２は、記録機器、１０３は、機器鍵記憶部、１０４は、入出力制御部、１０５は、コンテンツに施された暗号を復号する復号化部、１０６は、コンテンツ送受信先制限情報記憶部、１０７は、復号されたコンテンツデータを再生する再生処理部、１０８は、鍵暗号化データ記憶部、１０９は、メディア内送受信先制限情報記憶部、１１０は、入

出力制御部、１１１は、コンテンツ送受信先制限情報記憶部、１１２は、記録部である。

【００２６】以上のような構成において以下その動作を説明する。読み出し機器１０１内の機器鍵記憶部１０３は、図２における機器鍵記憶部３と同様機器に与えられた機器鍵を記憶する。

【００２７】記録機器１０２内のメディア鍵暗号化データ記憶部１０７およびメディア内送受信先制限情報記憶部１０８およびコンテンツ送受信先情報記憶部１０９は、図２の記録機器２におけるメディア鍵暗号化データ記憶部７およびメディア内送受信先制限情報記憶部８およびコンテンツ送受信先情報記憶部９と同等の機能をもち入出力制御部１１０により制御される。読み出し機器および記録機器間の送受信は、入出力制御部１０４および入出力制御部１１０で制御され行われる。

【００２８】図７は、読み出し機器および記憶機器間の処理のフローを説明した図である。同図において、３０１は、読み出しリクエスト送出処理、３０２は、鍵暗号化データリクエスト番号送出処理、３０３は、記録メディア鍵復号処理、３０４は、コンテンツ復号化鍵生成処理、３０５は、コンテンツ復号および再生処理、３０６は、コンテンツ送受信先制限情報読み取り処理、３０７は、リクエスト番号有効性確認処理、３０８は、メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理、３０９は、コンテンツデータ送出処理である。図７の左側の処理は、入出力制御部１０４、右側の処理が入出力制御部１１０の処理のフローである。まず、最初に、入力制御部１０４は、読み出しリクエスト信号送出処理３０１により、読み出したいデータを指定する。入力制御部１１０では、指定されたファイルのコンテンツ送受信先制限情報を読み取りコンテンツ送受信先制限情報記憶部１１１に記憶保持する。次に、入出力制御部１０４は、鍵暗号化データリクエスト番号送出処理３０２において、機器が保持する鍵のカテゴリー番号に相当する番号を入出力制御部１１０に送る。入出力制御部１１０は、リクエスト番号有効性確認処理３０７において、図６におけるリクエスト番号有効性確認処理２０７と同様にコンテンツ送受信先制限情報およびメディア送受信先制限情報から図８で説明した処理により送受信先制限情報Ｐｃｄを生成し、リクエスト番号がＰｃｄで許可されているかを確認判定し、否決の場合は、処理を停止し、許可されている場合は、メディア鍵暗号化データ送出処理３０８へ進む。メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理３０８では、リクエスト番号に対応する鍵番号に対応する暗号化データを鍵暗号化データ記憶部１０８より読み出し、入出力制御部１０４へコンテンツ送受信先制限情報とともに送る。入出力制御部１０４では、メディア鍵復号処理３０３において送られた暗号化データを機器鍵記憶部１０３の記憶する鍵で復号処理してメディア鍵Ｋｍを生成するとともに、コンテンツ送受信先制限情報コンテンツ送受信先制限情報記憶部１０６に記憶させる。続いて、コンテンツ鍵復号処理３０４において、メディア鍵Ｋｍとコンテンツ送受信先制限情報記憶部１０６内のコンテンツ送受信先制限情報に基づきコンテンツ復号鍵Ｋ＿ＣＯＮＴを生成し復号化処理部１０５にセットし、送信リクエスト信号を入出力制御部１１０へ送信する。入出力制御部１１０は、コンテンツデータ送信処理３０９で送信リクエストに応じてコンテンツデータを入出力制御部１０４に送信する。入力制御部１０４は、送信されてきたデータを復号処理部１０５に送り、暗号復号処理された後、再生部１０７で再生処理される。

【００２９】以上の処理により、データ読み取り機器３０１は、コンテンツおよび記録機器３０６にある送受信先制限情報により許可されているカテゴリーの機器鍵を持つ時のみデータを読み出すことができ、その他の許可のない機器がデータを読み出すことが困難にすることができる。特に記録機器内と記録されているデータにある両方の受信先制限情報に基づき行えるため、古い著作物で作成当時拒絶の対象とならなかったカテゴリー機器で不正が合った場合にその機器を記録機器にある送受信先制限情報に基づき読み出し困難にすることが出来る。

【００３０】図１０は、図１のような記述に基づき記録機器に記録し、図２、図３で説明したような読み取り機器、書き込み機器による記録機器への書き込みから読み出しまでの処理を説明した図である。同図において４０１は書き込み機器、４０２は、記録機器、４０３は、読み取り機器、４０４は暗号解読処理、４０５は、演算処理、４０６は、コンテンツ送受信制限情報、４０７は、コンテンツデータ、４０８は暗号化処理、４０９はｍメディア鍵暗号化データ、４１０は、送受信先制限情報、４１１は、メディア送受信制限情報、４１２は、コンテンツ送受信制限情報、４１３は、暗号化コンテンツデータ、４１４は、暗号復号化処理、４１５は、演算処理、４１６は、暗号復号化処理、４１７は、要素間のＯＲ処理である。

【００３１】コンテンツ４０７を記録機器に記録する場合、コンテンツ送受信先制限情報４０６を記録機器４０２に送信する。コンテンツ送受信先制限情報４１２は、メディア送受信制限情報４１１とＯＲ処理４１７で処理され、送受信先制限処理４１０に変換される。ここで、四角の箱が白である場所が許可されているカテゴリーとすると、コンテンツ側から1番目のと3番目が拒否され、記録機器から2番目が拒否され、結果4番目、5番目のカテゴリーのみが許可される。書き込み機器が、このカテゴリーの機器鍵を持っていたとすると、そのカテゴリー鍵に対応するメディア鍵暗号化データが書き込み機器４０１に送られ、暗号復号処理４０４にてメディア鍵Ｋｍが複製される。そのＫＭとコンテンツ送受信先制限情報４０６に基づき演算処理４０５でコンテンツ暗号用の鍵

が生成され、コンテンツを暗号化処理４０８で暗号化して記録メディアに送られ暗号コンテンツ４１３に送られ記録される。それを読み取り機器４０３が読み出す場合、記録機器４０２は、書き込み時の処理同じ手順で送受信先制限情報４１０に基づき読み取り機器側の機器鍵のカテゴリーが許可されているかを判定し、許可されている場合は、メディア鍵Ｋｍの暗号化データを送る。

【００３２】この場合、同じＫｍを暗号化しているため、書き込み機器内の機器鍵カテゴリーと読み取り機器内の機器鍵カテゴリーが異なってもかまわない。許可される場合、そのカテゴリに相当するものを送れば、読み取り機器側でＫｍを再生できる。そして、コンテンツ送受信制限情報４１２が読み取り機器に送られ、Ｋｍとともに演算処理ｆにより演算されてコンテンツ復号用の鍵が書き込み機器で暗号化したものと同じ値で生成される。したがって、暗号化コンテンツ４１３は、読み取り機器側で再生処理４１６により、正しく再生できる。

【００３３】以上のように、書き込み機器から読み取り機器へ記録機器を介してデータを送ることができ、その間の著作権情報である送受信先制限情報は、改ざんされない様に守れかつその情報が示す許可された機器に対して盗聴が困難なかたちで送受信することが出来る。

【００３４】なお、本実施の形態では、送受信先制限情報は許可不許可の表現を各カテゴリーに対して許可を０、不許可を１としたビット列で表現したが、それをランレングスコーディングしたものでもよいし、もっと別な変換処理した形式で表現してもよい。また、送信先制御情報を伝送する際、特に暗号化せずに送ったが、書き込み時に制限情報により不許可にならない様に送受信先制限情報を改ざんし、読み取り時に全く同じ改ざんを行われることで制限情報を回避させない様に、送信時、暗号化したり、チャックサムをつけて改ざんを検出可能にすることが出来る。

【００３５】また、暗号コンテンツの暗号部以外においても暗号処理を行っているのを図２、図３では入出力制御部で行っているが、これらは、通常暗号化データ数も少なく高速処理も要求されないのでソフトウエア的に十分可能であり、制御部内での処理として説明したが、それらの機器をハード的に構成することも可能である。また、図２、図３で示した構成以外でも同様の処理が可能な構成であればよい。

【００３６】また、メディア送信先制限情報とコンテンツ側の送信先制限情報をそれぞれ記憶部を設けて要素毎のＯＲ処理を施して最終的な制限情報を導き出したが、結果的にそれと同様のカテゴリーが不許可となるように判定できれば、他の方法でもよい。たとえば記録メディア送受信先制限情報は、鍵暗号化データ中から不許可部分のデータを抜き取ることで表現することもでき、それからコンテンツ送受信制御情報を使って同様の判定結果を得てもよい。

【００３７】また、本実施の形態では、送受信先制限情報からデータの暗号化鍵を生成させることで改ざんを防いでいるがデータに関連づける別の方法を用いても同様の効果選られる。たとえば、コンテンツデータを暗号化する暗号化鍵が別ファイルとして存在する場合は、そのファイル内のデータとしていっしょに記録するとともにファイル全体を改ざん防止のためのチェックサム等を用いることでコンテンツデータとの関連づけが可能となる。

【００３８】また、本実施の形態では、各カテゴリーの許可情報は、記録データの送受信先への許可情報としたが、それ以外の情報を意味するデータとして利用も可能である。たとえば、コピー禁止情報等のフラグとしても利用可能である。

【００３９】また、本実施の形態では、書き込み時についても制限情報を適応したが、読み込み時のみにこれを適応しただけでも書き込まれたデータを読み出すときに不正な機器での再生を困難にする効果を実現できる。

【００４０】また、本実施の形態で示した書き込み、読み出し手順以外でもコンテンツにある制限情報と記憶機器側にある制限情報に基づき送受信を制限するのであれば、その手続きなどの順番がことなってもよいし、異なる処理が挿入されてもよい。

【００４１】また、本実施の形態では、書き込み機器は、機器内の記録部にあるデータを記録機器に書き込んだが、書き込み機器に入力されてくるデータを記録機器に書き込む際にも同様に本発明を用いることが可能である。

【００４２】

【発明の効果】以上説明したように、本発明によれば、データを記録機器に書き込み読み出しする際に、記録機器内にある送受信先限定情報とデータに付加された送受信先限定情報によりデータの書き込み読み出しを制御するので双方の制限情報のうちより新しい情報に基づき不正機器を排除することができる。また、データに、付加する許可情報をデータの暗号化鍵の生成パラメータとして用いることで改ざんを防止するとともに、暗号化鍵生成パラメータとして記録機器にある鍵パラメータを用いることによりデータを復号するために必要なパラメータを記録データとは別に存在させることができ、単に通信路を盗聴しただけでは解読するための情報を入手できない様にすることができ、より不正が行うことが困難な著作権保護を実現できるデータ記録方法、読み出し方法および記録機器、読み出し機器、書き込み機器を提供することができ、本発明の実用的効果は大きい。

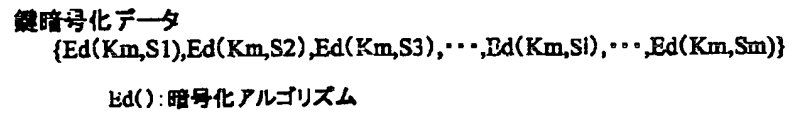
【図面の簡単な説明】

【図１】本実施の形態における記録データの記録時におけるデータ構成の説明図

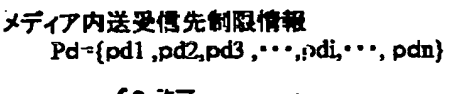
【図２】本発明の実施の形態における記録機器およびそれにデータを書き込む書き込み機器の構成図

【図３】本発明の実施の形態における記録機器からの読み出しを行う読み出し機器と記録機器の構成図
【図４】本発明の実施の形態におけるメディア鍵暗号化データの説明図
【図５】本発明の実施の形態におけるメディア内送受信先制限情報Ｐｄの説明図
【図６】本発明の実施の形態における入力制御部４および１０で行われる処理フローを示した説明図
【図７】本発明の実施の形態における読み出し機器および記憶機器間の処理のフローの説明図
【図８】本発明の実施の形態におけるコンテンツ送信先制限情報とメディア送受信先制限情報から送受信先の制限情報Ｐｄを算出する処理の説明図
【図９】本発明の実施の形態における送受信先制限情報Ｐｃｄの算出例の説明図
【図１０】本発明の実施の形態における読み取り機器、書き込み機器による記録機器への書き込みから読み出しまでの処理の説明図
【図１１】従来の記録および伝送時許可情報記述方法の説明図
【符号の説明】
１　データ書き込み機器
２　データ記録機器
３　機器鍵記憶部
４　入出力制御部
５　暗号化処理部
６　コンテンツ記録部
７　鍵暗号化データ記憶部
８　メディア内送受信先制限情報記憶部
９　コンテンツ送受信先制限情報記憶部
１０　書き込み機器との入出力制御部
１１　データ記録部
１０１　読み出し機器
１０２　記録機器
１０３　機器鍵記憶部
１０４　入出力制御部
１０５　コンテンツに施された暗号を復号する復号化部
１０６　コンテンツ送受信先制限情報記憶部
１０７　復号されたコンテンツデータを再生する再生処理部
１０８　鍵暗号化データ記憶部
１０９　メディア内送受信先制限情報記憶部
１１０　入出力制御部
１１１　コンテンツ送受信先制限情報記憶部
１１２　記録部
２０１　書き込みリクエストおよびコンテンツ送受信先制限情報送出処理
２０２　鍵暗号化データリクエスト番号送出処理
２０３　記録メディア鍵復号処理
２０４　コンテンツ暗号化鍵生成処理
２０５　コンテンツ暗号化送出処理
２０６　コンテンツ送受信先制限情報読み取り処理
２０７　リクエスト番号有効性確認処理
２０８　メディア鍵暗号化データ送出処理
２０９　コンテンツデータ記録処理
３０１　読み出しリクエスト送出処理
３０２　鍵暗号化データリクエスト番号送出処理
３０３　記録メディア鍵復号処理
３０４　コンテンツ復号化鍵生成処理
３０５　コンテンツ復号および再生処理
３０６　コンテンツ送受信先制限情報読み取り処理
３０７　リクエスト番号有効性確認処理
３０８　メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理
３０９　コンテンツデータ送出処理

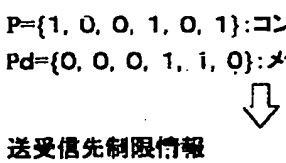
【図４】



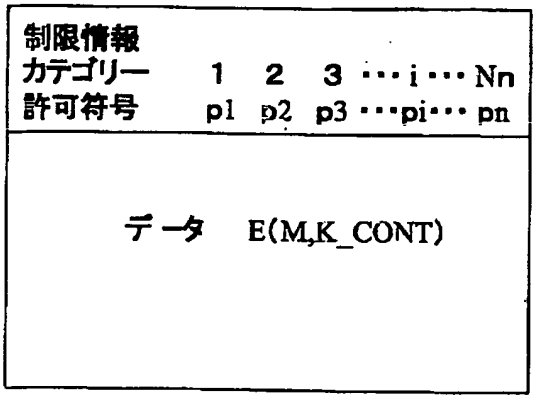
【図５】



【図９】

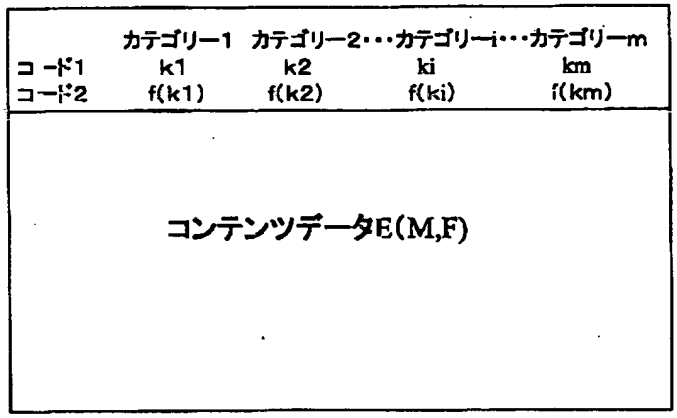


【図1】



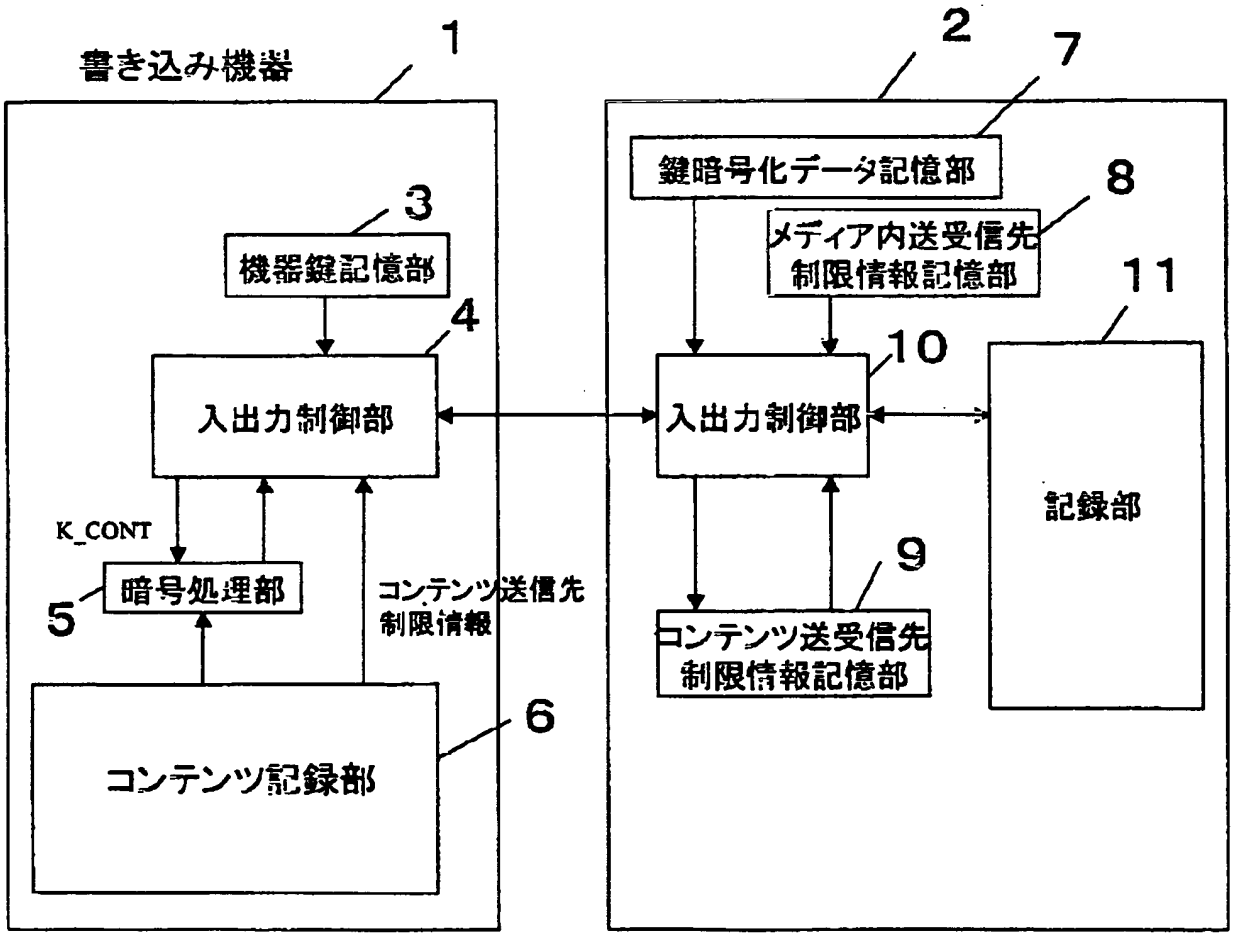
P={p1 ,p2,p3 ,・・・,pi,・・・, pn}:コンテンツ送受信先制限情報
K_CONT = f(P,K_m):コンテンツ暗号化鍵
f():コンテンツ鍵生成関数
pi = { 0 許可 / 1 不許可

【図11】

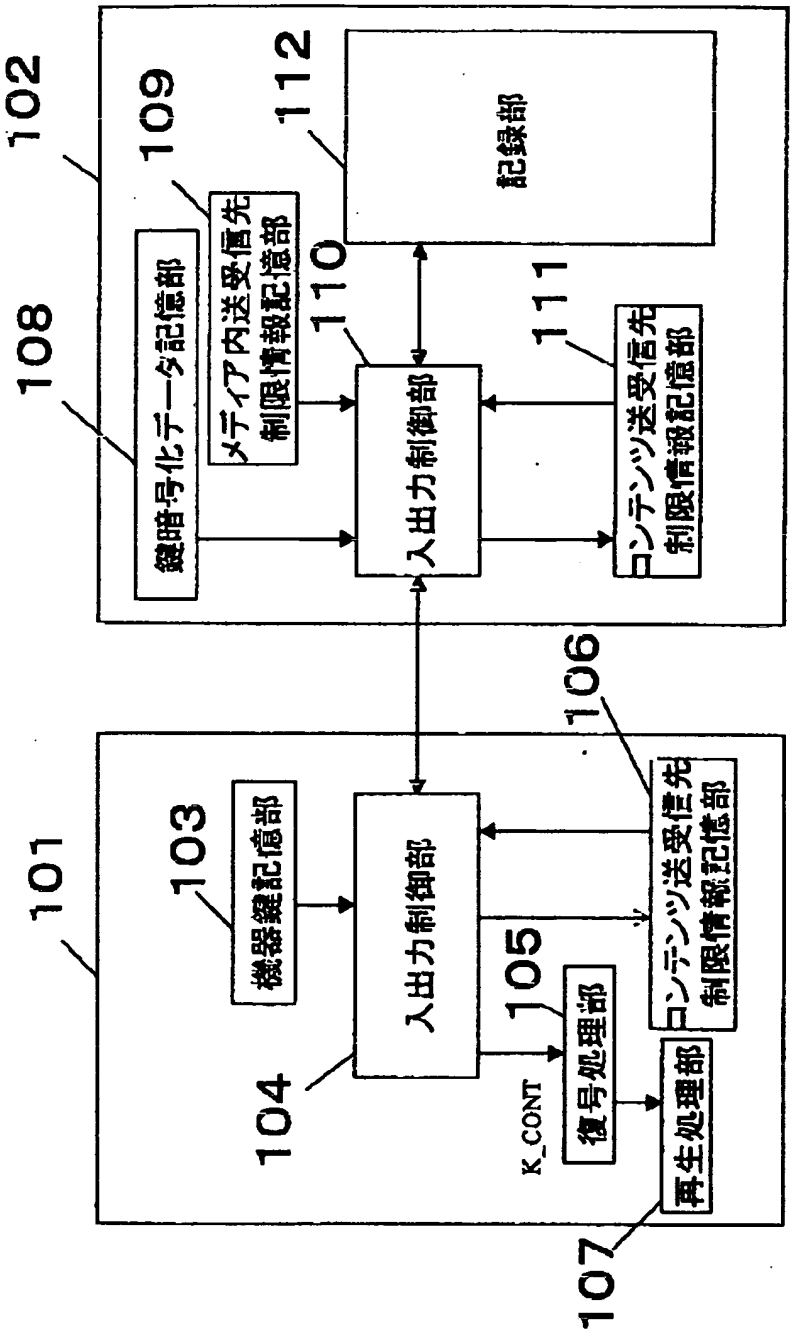


F:f(k1),f(k2),・・・f(ki),・・・,f(km)より計算される暗号化鍵
E():暗号処理

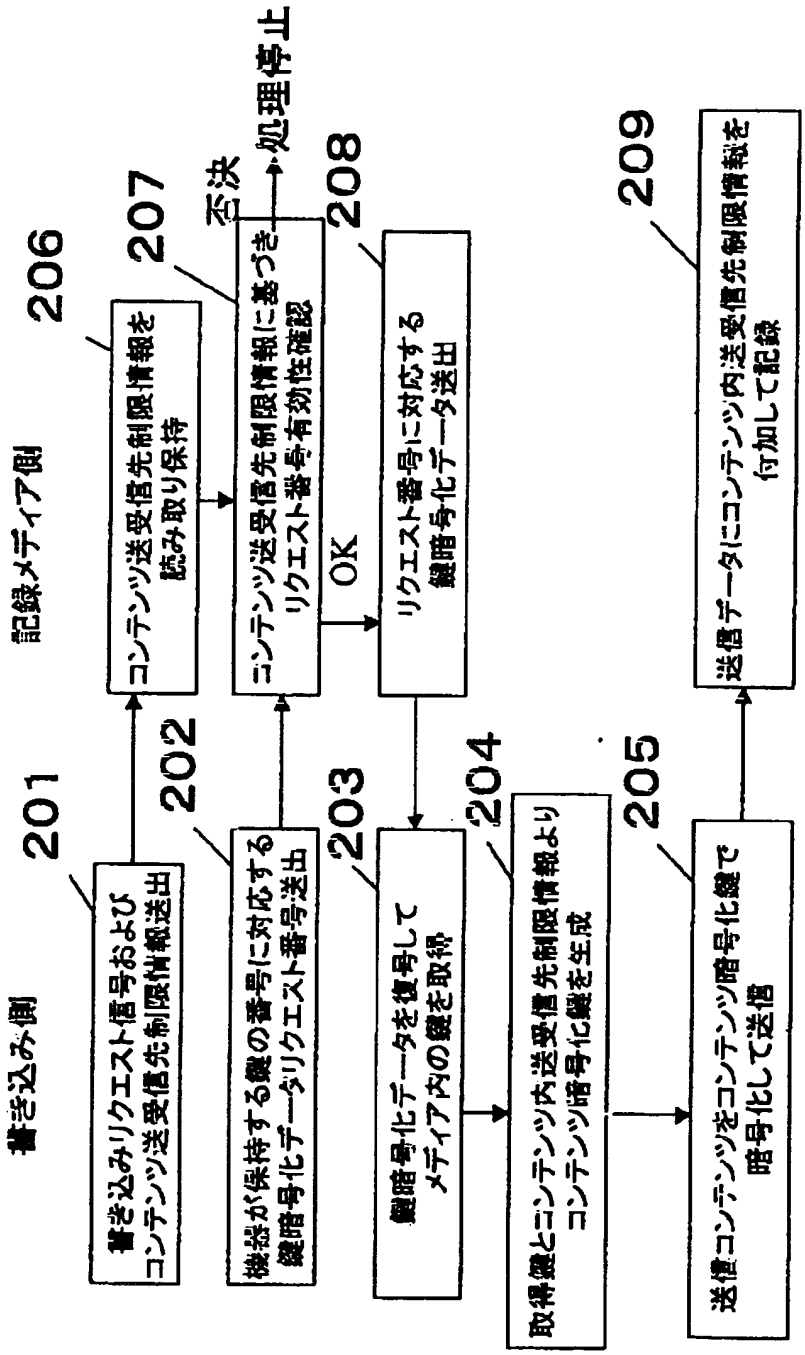
【図2】



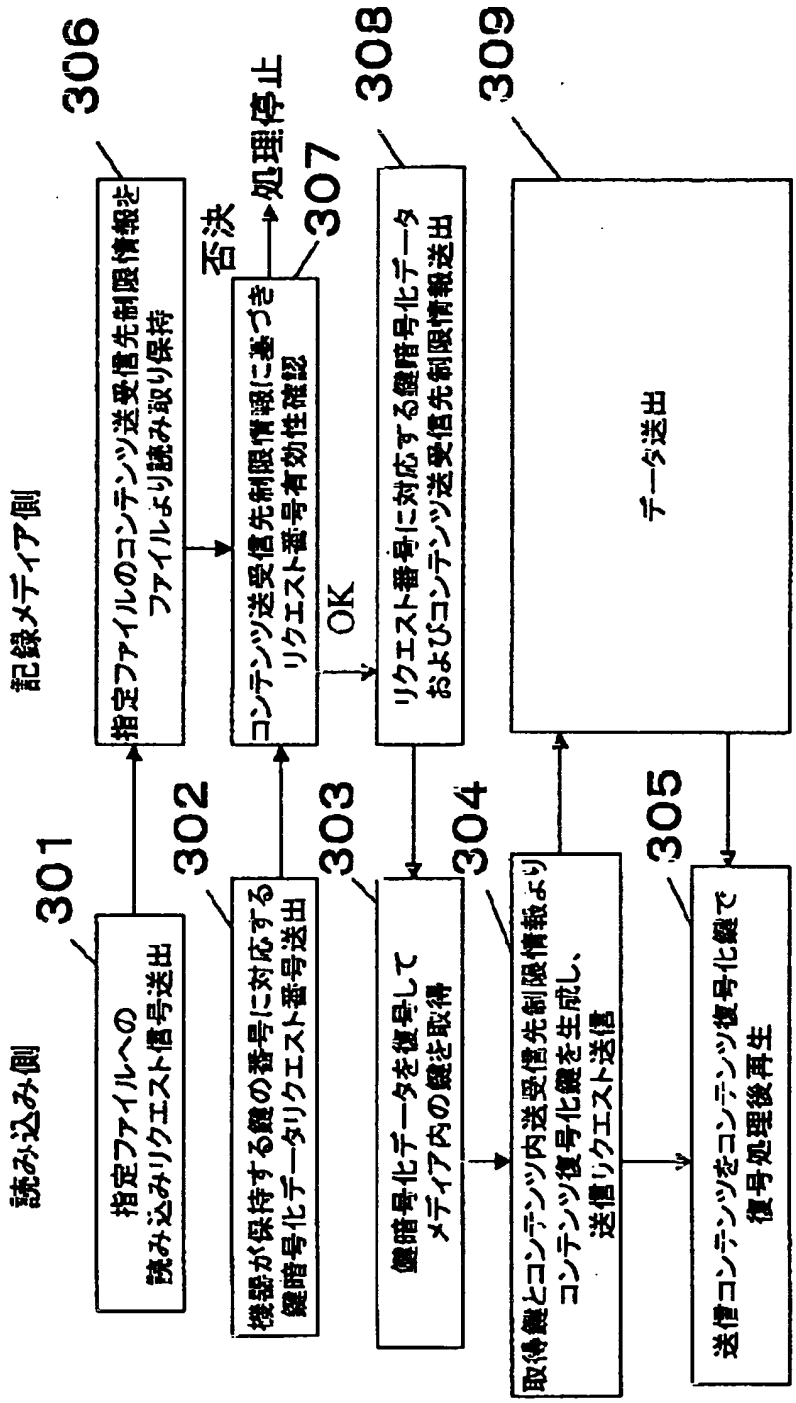
【図3】


102
109
112
記録部
メディア内送受信先制限情報記憶部
110
111
108
鍵暗号化データ記憶部
入出力制御部
コンテンツ送受信先制限情報記憶部
106
101
103
機器鍵記憶部
入出力制御部
コンテンツ送受信先制限情報記憶部
105
104
K_CONT
復号処理部
再生処理部
107

【図6】


書き込み側
記録メディア側
201
202
203
204
205
206
207
208
209
書き込みリクエスト信号およびコンテンツ送受信先制限情報送出
機器が保持する鍵の番号に対応する鍵暗号化データ要リクエスト番号送出
鍵暗号化データを復号してメディア内の鍵を取得
取得鍵とコンテンツ内送受信先制限情報よりコンテンツ暗号化鍵を生成
送信コンテンツをコンテンツ暗号化鍵で暗号化して送信
コンテンツ送受信先制限情報を読み取り保持
コンテンツ送受信先制限情報に基づきリクエスト番号有効性確認
否決
処理停止
OK
リクエスト番号に対応する鍵暗号化データ送出
送信データにコンテンツ内送受信先制限情報を付加して記録

【図7】


読み込み側
記録メディア側
301
指定ファイルへの
読み込みリクエスト信号送出
302
機器が保持する鍵の番号に対応する
鍵暗号化データリクエスト番号送出
303
鍵暗号化データを復号して
メディア内の鍵を取得
304
取得鍵とコンテンツ内送受信先制限情報より
コンテンツ復号化鍵を生成し、
送信リクエスト送信
305
送信コンテンツをコンテンツ復号化鍵で
復号処理後再生
306
指定ファイルのコンテンツ送受信先制限情報を
ファイルより読み取り保持
307
コンテンツ送受信先制限情報に基づき
リクエスト番号有効性確認
否決
処理停止
OK
308
リクエスト番号に対応する鍵暗号化データ
およびコンテンツ送受信先制限情報送出
309
データ送出

【図8】

P={p1 ,p2,p3 ,・・・,pi,・・・, pn}:コンテンツ送受信先制限情報

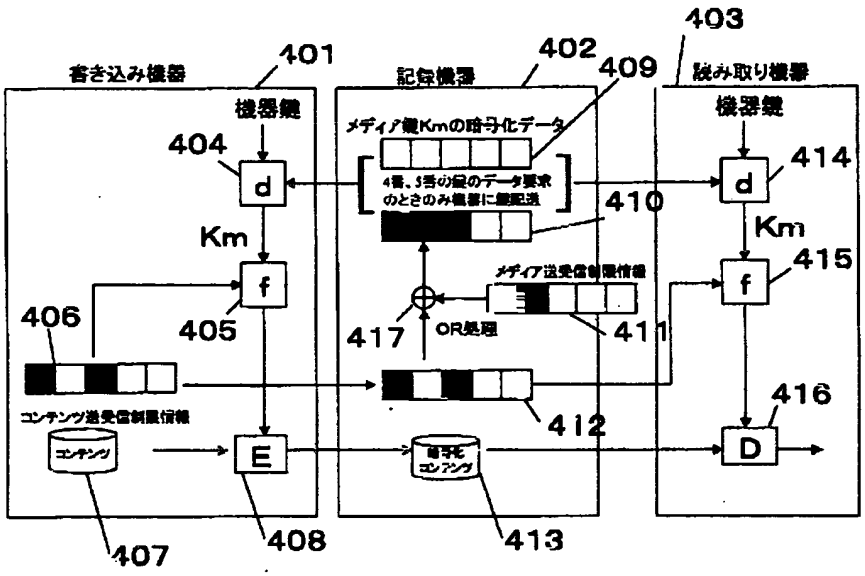
Pd={pd1 ,pd2,pd3 ,・・・,pdi,・・・, pdn}:メディア送受信先制限情報

⇩

送受信先制限情報
Pcd={pd1^p1 ,pd2^p2,pd3^p2 ,・・・,pdi^pi,・・・, pdn^pn}

^:OR処理

【図10】



フロントページの続き

(72)発明者 原田 俊治
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 館林 誠
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B017 AA06 BA04 BA05 BA07 BB02
BB03 CA07 CA14 CA16
5B025 AD14 AE10
5B065 PA04 PA16
5D044 DE17 DE50 EF05 FG18 GK12
GK17
5J104 AA07 AA13 AA16 AA41 EA18
GA05 KA02 NA03 NA27 PA14